UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/755,195	01/31/2013	Siva Raj Rajagopalan	83138407	7989

56436 7590 01/11/2017

Hewlett Packard Enterprise
3404 E. Harmony Road
Mail Stop 79
Fort Collins, CO 80528

EXAMINER	
DADA, BEEMNET W	

ART UNIT	PAPER NUMBER
2435	

NOTIFICATION DATE	DELIVERY MODE
01/11/2017	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

hpe.ip.mail@hpe.com
chris.mania@hpe.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte SIVA RAJ RAJAGOPALAN, TOMAS SANDER, and SURANJAN PRAMANIK

Appeal 2016-000762
Application 13/755,195[1]
Technology Center 2400

Before BRUCE R. WINSOR, NABEEL U. KHAN, and MICHAEL J. ENGLE, *Administrative Patent Judges*.

ENGLE, *Administrative Patent Judge*.

DECISION ON APPEAL

Appellants appeal under 35 U.S.C. § 134(a) from a final rejection of claims 1–15, which are all of the claims pending in the application. We have jurisdiction under 35 U.S.C. § 6(b).

We AFFIRM-IN-PART.

Technology

The application relates to security threat analysis. Abstract. Claim 1 is illustrative and reproduced below with the limitations at issue emphasized:

---

[1] According to Appellants, the real party in interest is Hewlett-Packard Development Company, LP, which is wholly-owned by Hewlett-Packard Company. App. Br. 3.

1. A method for security threat analysis, comprising:

utilizing a processor to execute instructions stored on a non-transitory medium for:

generating a security related task based on security data in a security monitoring server, wherein the security related task includes an analysis of data and the security data is received via communications links from a plurality of security monitored participants;

sending, via a communication link, *to at least one of the plurality of security monitored participants*:

a request to complete the security related task based on the at least one security monitored participant's ability to carry out the task, and

a set of the security data, wherein the set of security data is from at least two of the plurality of security monitored participants; and

receiving a response from the at least one security monitored participant with information related to the security related task.

Rejection

Claims 1–15 stand rejected under 35 U.S.C. § 103(a) as obvious over the combination of Zheng et al. (US 8,065,725 B2; Nov. 22, 2011) and Njemanze et al. (US 8,056,130 B1; Nov. 8, 2011). Final Act. 2.

ISSUES

1. Did the Examiner err finding Zheng teaches or suggests sending a request "based on the . . . ability to carry out the task" (claim 1), "based on the processed security data" (claim 6), or "based on the pattern" (claim 11)?

2. Did the Examiner err finding the combination of Zheng and Njemanze teaches or suggests "to verify the security threat hypothesis," as recited in claims 6 and 11?

3. Did the Examiner err finding Zheng teaches or suggests "a security monitored participant," as recited in claims 1, 6, and 11?

4. Did the Examiner err finding Zheng teaches or suggests "sending the request to a subset of the plurality of security monitored participants, the subset having a similar pattern in their corresponding security data," as recited in claim 3?

ANALYSIS

Independent Claims 1, 6, and 11

The three independent claims (1, 6, and 11) recite similar but slightly different requirements for sending a request. Claim 1 recites "sending . . . to at least one of the plurality of security monitored participants: a request to complete the security related task *based on the at least one security monitored participant's ability to carry out the task*."

Independent claim 6 sends a request "*based on the processed security data* for an analysis to verify the security threat hypothesis."

Independent claim 11 sends a request "*based on the pattern* for analysis to verify the security threat hypothesis."

The Examiner relies primarily on Zheng for teaching these limitations. Zheng teaches an intrusion detection system that includes "normal nodes," which perform tasks required for intrusion detection, and "supernodes," which "perform[] higher-level functions compared to a normal node." Zheng 6:37–50. "The primary purpose of a supernode is to perform analysis of data captured by other nodes, both normal and supernodes." *Id.* at 6:48–50. For example, groups of normal nodes called "collectives" may "send their results to the supernode collective, where higher-level correlation can be performed" and the supernode collective then may be able to correlate an

"entire chain of attacks" rather than the individual pieces seen by each normal collective. *Id.* at 25:55–67.

Appellants first contend that data is not sent to a supernode "based on the [supernode's] ability to carry out the task" for claim 1. App. Br. 7–8. However, Appellants have not sufficiently addressed the Examiner's finding that a normal node forwards data to a supernode because the supernode "performs higher level functions (i.e., capable of carrying out the task)." Ans. 3 (citing Zheng 6:37–53, 25:55–26:2).

Similarly, Appellants have not sufficiently persuaded us against the Examiner's finding that the data is sent to the supernode "based on the processed security data" (claim 6) or "based on the pattern" (claim 11). *Id.* For example, in the cited example of Zheng, "Collective A [of normal nodes] is able to identify the chain of logins [i.e., 'potential attacks'] from Nodes A4, A1, and A2. Collective A would then submit its findings to the supernode collective." Zheng 25:55–61. "The collectives send their results to the supernode collective, where higher-level correlation can be performed." *Id.* at 25:63–65. Thus, the data regarding logins is sent to the supernode because the logins may indicate a potential attack and require further analysis (i.e., "based on the processed security data" or "based on the pattern").

Appellants further contend the data is not sent "to verify the security threat hypothesis," as recited in claims 6 and 11. App. Br. 8–9. We are not persuaded for the same reasons discussed above, namely that the data is sent to the supernode because there is a hypothesis that needs further analysis (e.g., whether the detected logins are an indication of an attack). *See* Ans. 4. The Examiner also relies on a combination with Njemanze, which teaches a

similar process of agents notifying managers of events for further cross-correlation. *Id.* (citing Njemanze 9:39–10:25). Here, the prior art need not use identical language as the claim to render the claim obvious (i.e., there is no *ipsissimis verbis* test). *See In re Gleave*, 560 F.3d 1331, 1334 (Fed. Cir. 2009).

Appellants also argue "a security monitored participant [as claimed] is not analogous to a supernode [as taught by Zheng]." Reply Br. 3. However, Appellants have not adequately explained this assertion, nor provided any definition for the term. The Specification teaches:

> A threat exchange community can be a group of computing systems that exchange information related to information technology infrastructures . . . . The computing systems can be referred to as *participants* of the threat exchange community. In some implementations, *entities including or controlling the computing systems can also be referred to as participants* of the threat exchange community.

Spec. ¶ 8 (emphasis added). Zheng's supernodes are part of a threat exchange community and receive information from both normal nodes and other supernodes. Zheng 6:44–50. Given the Specification's broad description of participants, Appellants have not persuaded us of error in the Examiner finding Zheng's supernodes are "security monitored participants."

Accordingly, we sustain the Examiner's rejection of claims 1, 6, and 11, and claims 2, 5, 7–10, and 12–15, which Appellants argue are patentable for similar reasons. *See* App. Br. 10; 37 C.F.R. § 41.37(c)(1)(iv).[2]

---

[2] In the event of further prosecution, the Examiner may wish to consider whether at least independent claims 1, 6, and 11 are patentable under 35 U.S.C. § 101 in light of *Alice Corp. v. CLS Bank Int'l*, 134 S. Ct. 2347, 2352 (2014) and recent Federal Circuit precedent applying *Alice*. For example, other than the use of a generic processor, claim 1 may be met by a team of

Dependent Claim 3

Claim 3 depends from claim 1 and further recites "sending the request to *a subset* of the plurality of security monitored participants, the subset having *a similar pattern in their corresponding security data*."

The Examiner relies on Zheng for this limitation. Final Act. 4 (citing Zheng 25:55–26:2); Ans. 4. Appellants contend that in Zheng, it is the supernode that "determines if the collectives have similar patterns," so there is no way to know before the supernode's analysis whether the data sent to the supernode has similar patterns. App. Br. 10. Appellants further contend "data from multiple lower nodes . . . does not include 'corresponding security data' related to the supernode itself." Reply Br. 5.

Although we do not agree with all of Appellants' arguments, we are persuaded by Appellants' argument that the Examiner has not shown "corresponding security data" related to the supernode. For claim 1, the Examiner relied on the request being sent to a supernode for further analysis. A supernode can receive data from both normal nodes and other supernodes. Zheng 6:48–50. A "subset" could be just one node (e.g., one supernode receiving data). However, the subset must have "a similar pattern in their corresponding security data." The Examiner has not sufficiently explained whether a supernode receiving data from other nodes has its own "corresponding security data," nor identified what the "similar pattern" in Zheng would be. As the Supreme Court and Federal Circuit have said, "there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." *In re Kahn*, 441 F.3d 977,

---

police officers at a crime scene providing what they find to the detectives for further analysis.

988 (Fed. Cir. 2006); *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007) (quoting *Kahn*). "The pertinence of each reference, if not apparent, must be clearly explained." 37 C.F.R. § 1.104(c)(2). The Examiner has not sufficiently done so here.

Accordingly, we do not sustain the Examiner's rejection of claim 3, or claim 4, which depends from claim 3.

DECISION

For the reasons above, we affirm the Examiner's decision rejecting claims 1, 2, and 5–15, but reverse the Examiner's decision rejecting claims 3 and 4.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a). *See* 37 C.F.R. § 41.50(f).

AFFIRMED-IN-PART